

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of : THE COMMISSIONER IS AUTHORIZED
Masaki YAMAUCHI et al. : TO CHARGE ANY DEFICIENCY IN THE
Serial No. NEW : FEES FOR THIS PAPER TO DEPOSIT
Filed July 29, 2003 : ACCOUNT NO. 23-0975
: Attn: APPLICATION BRANCH
: Attorney Docket No. 2003_1057A

AUTHENTICATION APPARATUS
AND AUTHENTICATION METHOD

CLAIM OF PRIORITY UNDER 35 USC 119

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants in the above-entitled application hereby claim the date of priority under the International Convention of Japanese Patent Application No. 2002-226532, filed August 2, 2002, as acknowledged in the Declaration of this application.

A certified copy of said Japanese Patent Application is submitted herewith.

Respectfully submitted,

Masaki YAMAUCHI et al.

By



W. Douglas Hahm

Registration No. 44,142 *for*

Michael S. Huppert

Registration No. 40,268

Attorney for Applicants

MSH/kjf
Washington, D.C. 20006-1021
Telephone (202) 721-8200
Facsimile (202) 721-8250
July 29, 2003

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application: 2002年 8月 2日

出願番号

Application Number: 特願2002-226532

[ST.10/C]:

[JP2002-226532]

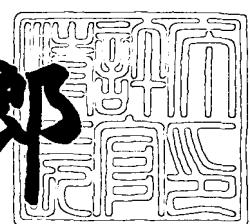
出願人

Applicant(s): 松下電器産業株式会社

2003年 3月14日

特許庁長官
Commissioner,
Japan Patent Office

太田 信一郎



出証番号 出証特2003-3017284

【書類名】 特許願
【整理番号】 2022540089
【あて先】 特許庁長官殿
【国際特許分類】 H04Q 7/34
G01C 21/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内
【氏名】 山内 真樹

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内
【氏名】 岡林 一郎

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 森 康浩

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 川端 章裕

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式
会社内

【氏名】 余田 貞人

【特許出願人】

【識別番号】 000005821
【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【電話番号】 06-4806-7530

【手数料の表示】

【予納台帳番号】 049515

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証装置及び認証方法

【特許請求の範囲】

【請求項1】 特定の個体を対象として、その正当性を認証する認証装置であって、

前記個体から、当該個体を特徴づける第1対象情報を取得する対象情報取得手段と、

前記取得された第1対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、

前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加手段と

を備えることを特徴とする認証装置。

【請求項2】 前記認証装置は、さらに、
前記特定の個体を認識するための第2対象情報を予め記憶している記憶手段を備え、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る第2対象情報を読み出し、当該第2対象情報と前記取得された第1対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証する
ことを特徴とする請求項1記載の認証装置。

【請求項3】 前記特定の個体は、特定の個人である
ことを特徴とする請求項1又は2記載の認証装置。

【請求項4】 前記対象情報取得手段は、
前記第1対象情報として、前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の情報を取得し、
前記対象情報認証手段は、

前記取得された第1対象情報に基づいて、前記認証を行なう
ことを特徴とする請求項3記載の認証装置。

【請求項5】 前記特定の個体は、特定の個人及び当該個人が所持する物品

である

ことを特徴とする請求項1又は2記載の認証装置。

【請求項6】 前記対象情報取得手段は、

前記第1対象情報として、前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表わす対象情報のうち、少なくとも一の情報を取得し、かつ前記物品を特徴付ける識別コード及び当該物品の外観を表わす対象情報のうち、少なくとも一の対象情報を取得し、

前記対象情報認証手段は、

前記取得された第1対象情報に基づいて、重畠して前記認証を行なうこと

ことを特徴とする請求項5記載の認証装置。

【請求項7】 前記位置情報付加手段は、

G P S (Global Positioning System) によって、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項1又は2記載の認証装置。

【請求項8】 前記位置情報付加手段は、P H S (Personal Handyphone System) 又は携帯電話システムの基地局から、前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項1又は2記載の認証装置。

【請求項9】 前記認証装置は、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記位置情報付加手段は、さらに、

前記時計から前記個体が存在する時刻を表わす時間情報を取得して付加する

ことを特徴とする請求項1～8項の何れか1項に記載の認証装置。

【請求項10】 前記位置情報付加手段は、さらに、

電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して付加する

ことを特徴とする請求項1～8項の何れか1項に記載の認証装置。

【請求項11】 特定の個体を対象として、その正当性と当該個体が実存することを認証する認証装置であって、

前記個体を特徴づける対象情報を取得する対象情報取得手段と、
前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、
前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認
証手段と、
前記取得された位置情報に基づいて、前記個体が存在する位置を認証する位置
情報認証手段と、
前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が
実存すると認証する実存認証手段と
を備えることを特徴とする認証装置。

【請求項12】 前記認証装置は、さらに、
前記特定の個体を認識するための第2対象情報を予め記憶している記憶手段を
備え、
前記対象情報認証手段は、
前記記憶手段から、前記特定の個体に係る第2対象情報を読み出し、当該第2
対象情報と前記取得された第1対象情報とを照合し、その結果が一致した場合に
、前記特定の個体が正当であると認証する
ことを特徴とする請求項11記載の認証装置。

【請求項13】 前記特定の個体は、特定の個人及び当該個人が所持する物
品である

ことを特徴とする請求項11又は12記載の認証装置。

【請求項14】 前記対象情報取得手段は、
前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表
わす対象情報のうち、少なくとも一の対象情報を取得し、かつ前記物品を識別し
得る識別コード及び当該物品の外観を表わす対象情報を取得し、
前記対象情報認証手段は、
前記取得された対象情報に基づいて、重複して前記認証を行なう
ことを特徴とする請求項13記載の認証装置。

【請求項15】 前記位置情報取得手段は、
GPS (Global Positioning System) によって、前記個体が存在する位置の

位置情報を取得する

ことを特徴とする請求項11又は12記載の認証装置。

【請求項16】 前記位置情報取得手段は、

PHS (Personal Handyphone System) 又は携帯電話システムの基地局から、

前記個体が存在する位置の位置情報を取得する

ことを特徴とする請求項11又は12記載の認証装置。

【請求項17】 前記認証装置は、さらに、

前記個体が存在した時刻を表わす時間情報を取得する時間情報取得手段と、

前記取得された時間情報に基づいて、前記個体が存在した時刻を認証する時間情報認証手段とを備え、

前記実存認証手段は、さらに、

前記認証された時刻において前記個体が実存すると認証する

ことを特徴とする請求項15又は16項に記載の認証装置。

【請求項18】 前記認証装置は、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記時間情報認証手段は、さらに、

前記内蔵する時計から前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項17記載の認証装置。

【請求項19】 前記時間情報認証手段は、さらに、

電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項17記載の認証装置。

【請求項20】 前記認証装置は、さらに、

前記特定の個体を特徴づける対象情報と、当該個体が所定の予定に従って移動された場合における移動後の位置及び時刻を表わす位置情報及び時間情報とを予め記憶する記憶手段を備え、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る対象情報を読み出し、当該読み出さ

れた対象情報と前記取得された対象情報とを照合し、その結果が一致した場合に

、前記特定の個体が正当であると認証し、

前記位置情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の位置情報を読み出し、

当該読み出された位置情報と前記取得された位置情報を照合し、その結果が一

致した場合に、前記特定の個体が存在する位置が正当であると認証し、

前記時間情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の時間情報を読み出し、

当該読み出された時間情報と前記取得された時間情報を比較し、それらが同じ

時間帯であると判定された場合に、前記特定の個体が存在する時刻が正当である

と認証する

ことを特徴とする請求項18又は19記載の認証装置。

【請求項21】 特定の個人及び当該個人が所持する特定の物品のうち、少なくとも一つの個体を対象として、当該個体の正当性と当該個体が実存することを認証するための認証サーバと、当該認証サーバにネットワークを介して接続されている認証用端末とからなる認証システムであって、

前記認証用端末は、

前記個体から、当該個体を特徴づける対象情報を取得する対象情報取得手段と

前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、

取得された前記対象情報及び前記位置情報を前記認証サーバに送信する送信手段とを備え、

前記認証サーバは、

前記認証用端末から対象情報及び位置情報を受信する受信手段と、

前記受信された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証手段と、

前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が

実存すると認証する実存認証手段とを備える
ことを特徴とする認証システム。

【請求項22】 前記認証用端末の前記対象情報取得手段は、
前記特定の個人を識別し得るパスワード、指紋、声紋、顔の外観及び虹彩を表
わす対象情報のうち、少なくとも一の対象情報を取得し、前記物品を識別し得る
識別コード及び当該物品の外観を表わす対象情報のうち、少なくとも一の対象情
報を取得し、

前記認証サーバの前記対象情報認証手段は、
前記受信された対象情報に基づいて、重畠して前記認証を行なう
ことを特徴とする請求項21記載の認証システム。

【請求項23】 前記認証用端末の前記位置情報取得手段は、
G P S (Global Positioning System) によって、前記個体が存在する位置の
位置情報を取得する
ことを特徴とする請求項21記載の認証システム。

【請求項24】 前記認証用端末の前記位置情報取得手段は、
P H S (Personal Handyphone System) 又は携帯電話システムの基地局から、
前記個体が存在する位置の位置情報を取得する
ことを特徴とする請求項21記載の認証システム。

【請求項25】 前記認証用端末は、さらに、
前記個体が存在した時刻を表わす時間情報を取得する時間情報取得手段を備え
前記送信手段は、前記取得された時間情報をも前記認証サーバに送信し、
前記認証サーバの前記受信手段は、さらに、前記認証用端末から時間情報を受
信し、

前記認証サーバは、さらに、
受信された前記時間情報に基づいて、前記個体が存在した時刻を認証する時間
情報認証手段とを備え、

前記実存認証手段は、さらに、
前記認証された時刻において前記個体が実存すると認証する

ことを特徴とする請求項23又は24記載の認証システム。

【請求項26】 前記認証サーバは、さらに、年月日字分秒を計時し得る時計を内蔵し、

前記時間情報認証手段は、さらに、

前記内蔵する時計から前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項25記載の認証システム。

【請求項27】 前記認証サーバの前記時間情報認証手段は、さらに、電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して認証する

ことを特徴とする請求項25記載の認証システム。

【請求項28】 前記認証サーバは、さらに、前記特定の個体を特徴づける対象情報と、当該個体が所定の予定に従って移動された場合における移動後の位置及び時刻を表わす位置情報及び時間情報とを予め記憶する記憶手段を備え、

前記認証サーバにおいて、

前記対象情報認証手段は、

前記記憶手段から、前記特定の個体に係る対象情報を読み出し、当該読み出された対象情報と前記受信された対象情報とを照合し、その結果が一致した場合に、前記特定の個体が正当であると認証し、

前記位置情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の位置情報を読み出し、当該読み出された位置情報と前記受信された位置情報とを照合し、その結果が一致した場合に、前記特定の個体が存在する位置が正当であると認証し、

前記時間情報認証手段は、

前記記憶手段から、前記特定の個体に係る前記移動後の時間情報を読み出し、当該読み出された時間情報と前記受信された時間情報とを比較し、それらが同じ時間帯であると判定された場合に、前記特定の個体が存在する時刻が正当であると認証する

ことを特徴とする請求項26又は27記載の認証装置。

【請求項29】 前記認証用端末の送信手段は、さらに、
認証用端末を識別し得る情報を、前記対象情報及び前記位置情報に付加して前
記認証サーバに送信し、

前記認証サーバの受信手段は、さらに、

前記受信した認証用端末を識別し得る情報が正当か否かを判別し、正当な情報
であると判別された場合に、前記受信した対象情報及び位置情報を有効な情報と
して扱う

ことを特徴とする請求項28記載の認証システム。

【請求項30】 前記認証サーバは、さらに、
前記受信した認証用端末を識別し得る情報が正当な情報でないと判別された場
合に、当該認証用端末に所定の警告を表わす情報を送信する警告送信手段を備え

前記認証用端末は、さらに、

前記認証サーバから、前記警告を表わす情報を受信し、当該情報の内容を提示
する警告受信手段を備える

ことを特徴とする請求項29記載の認証システム。

【請求項31】 前記認証用端末の送信手段は、さらに、
前記対象情報及び前記位置情報を暗号化して前記認証サーバに送信し、
前記認証サーバの受信手段は、さらに、
前記認証用端末から受信した暗号化された対象情報及び位置情報を復号する
ことを特徴とする請求項29記載の認証システム。

【請求項32】 前記認証サーバは、さらに、
所定の規則に基づいて、前記認証用端末を識別し得る情報を更新して前記認証
用端末に通知し、

前記認証用端末は、さらに、
所定の規則に基づいて、前記認証サーバから通知により、前記認証用端末を識
別し得る情報を更新する

ことを特徴とする請求項29記載の認証システム。

【請求項33】 特定の作業員の正当性と当該作業員が存在する位置を把握して所定の施設における施錠を管理する管理サーバと、当該管理サーバにネットワークを介して接続されている作業員端末とからなる施錠管理システムであって

前記作業員端末は、

前記作業員から、当該作業員を特徴づける対象情報を取得する対象情報取得手段と、

前記作業員が存在する位置を表わす位置情報を取得する位置情報取得手段と、

取得された前記対象情報及び前記位置情報を前記管理サーバに送信する送信手段とを備え、

前記管理サーバは、

前記作業員端末から対象情報及び位置情報を受信する受信手段と、

前記受信された対象情報に基づいて、前記作業員の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記作業員が存在する位置が安全な位置か否かを判別する位置情報判別手段と、

前記作業員の正当性が認証され、前記作業員の位置が安全な位置であると判別された場合に、前記所定の施設に施錠を行なう

ことを特徴とする施錠管理システム。

【請求項34】 特定の社員の正当性と当該社員が存在する位置と時刻とを把握して所定の訪問先に対する巡回訪問を管理する管理サーバと、当該管理サーバにネットワークを介して接続されている社員端末とからなる巡回管理システムであって、

前記社員端末は、

前記社員から、当該社員を特徴づける対象情報を取得する対象情報取得手段と

前記社員が存在する位置を表わす位置情報を取得する位置情報取得手段と、

前記社員が存在する時刻を表わす時間情報を取得する時間情報取得手段と、

取得された前記対象情報、前記位置情報及び前記時間情報を前記管理サーバに

送信する送信手段とを備え、

前記管理サーバは、

前記社員端末から前記対象情報、前記位置情報及び前記時間情報とを受信する受信手段と、

前記受信された対象情報に基づいて、前記社員の正当性を認証する対象情報認証手段と、

前記受信された位置情報に基づいて、前記社員が存在する位置が正当な訪問先の位置か否かを判別する位置情報判別手段と、

前記受信された時間情報に基づいて、前記社員が存在する時刻が正当な時間か否かを判別する時間情報判別手段と、

前記社員の正当性が認証され、前記社員の位置及び時間が正当な位置及び時間であると判別された場合に、前記巡回訪問は正当であると判定することを特徴とする巡回管理システム。

【請求項35】 特定の個体を対象として、その正当性を認証する認証方法であって、

前記個体から、当該個体を特徴づける第1対象情報を取得する対象情報取得ステップと、

前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証ステップと、

前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加ステップと

を有することを特徴とする認証方法。

【請求項36】 特定の個体を対象として、その正当性と当該個体が実存することを認証する認証方法であって、

前記個体を特徴づける対象情報を取得する対象情報取得ステップと、

前記個体が存在する位置を表わす位置情報を取得する位置情報取得ステップと

前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証ステップと、

前記取得された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証ステップと、

前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が実存すると認証する実存認証ステップと
を有することを特徴とする認証方法。

【請求項37】 特定の個体を対象として、その正当性を認証する認証装置のためのプログラムであって、

請求項35記載の認証方法に含まれる全てのステップをコンピュータに実行させることを特徴とするプログラム。

【請求項38】 特定の個体を対象として、その正当性と当該個体が実存することを認証する認証装置のためのプログラムであって、

請求項36記載の認証方法に含まれる全てのステップをコンピュータに実行させることを特徴とするプログラム。

【発明の詳細な説明】

【発明の属する技術分野】

本発明は、特定の個人や特定の物品を対象とする認証装置に関する。特に、それらの対象が、特定の位置や特定の時間に存在する場合についても認証し得る認証装置に関する。

【0001】

【従来の技術】

従来、「特定の位置」に「特定の個体（人や物）」が「存在すること／存在したこと」を管理したい場合がある。例えば、営業マンの外回りの活動をその上司が管理する「巡回管理」が該当する。この場合、従来の技術では、G P S端末や携帯電話等を営業マンに携帯させ、G P Sや携帯電話の基地局から送信される位置情報等に基づいて「位置追跡」や「位置特定」を行ない、その位置情報等を上司が使用する管理サーバに送信させることによって、上記の管理を行なっている。

【0002】

また、例えば、特開2000-209641号公報記載の「位置情報通信シス

テム」（従来例1）や、特表2001-503134号公報記載の「地理データマネージャ」（従来例2）や、特開2001-91291号公報記載の「情報処理装置」（従来例3）や、特開2000-354268号公報記載の「ロケーション管理システム」（従来例4）等の場合は、所定の端末の位置情報に基づいて位置の確認／特定が可能である。さらに、特開2000-197098号公報記載の「位置情報管理装置」（従来例5）は、位置情報の通知機能を有する端末同士での位置情報の共有が可能である。さらにまた、特開2000-304564号公報記載の「探索用携帯端末機」（従来例6）は、特定の個人（徘徊者）の位置情報を入手することができる。

【0003】

さらに、特開2001-119761に記載の「情報提供システム」（従来例7）は、端末利用者が所定の場所に行ったときにその利用者が予め要求していた情報を得ることができる。さらに、特開2001-36840号公報記載の「撮影画像管理方法」（従来例8）は、デジタルカメラで撮影された画像にその撮像場所情報を添付することができる。

なお、上記の声紋データを用いる認証方法については、特開平8-223281「携帯電話機」等に記載されている。また、顔の特徴を表わした画像データを用いる認証方法については、特開平11-85988「顔画像認識システム」等に記載されている。さらにまた、虹彩データを用いる認証方法については、特開平9-212644「虹彩認識装置及び虹彩認識方法」等に記載されている。

【0004】

【発明が解決しようとする課題】

しかしながら、これらの従来例は、特定の人物に1対1に対応して装置が与えられ、その装置に位置情報を送信することが絶対条件となっている。そのため、「特定の人物以外によって端末が特定の位置まで運ばれた場合」といった「なりすまし」的ケースに対して全く無力である。

また、「特定の位置（場所）」に「特定の個体」が存在すること（存在したこと）を認識したい状況において、「特定の個体」が認識したい側からみて「不特定多数」である場合にも無力である。つまり、特定の個体と従来の機器が1対1

に対応していない場合、従来の機器では認証そのものが不可能である。言い換えると、「位置（場所）」と「個体」の双方を認証できる端末装置、もしくは端末装置とサーバ装置からなるシステムが存在していないために、これらの問題が起こっている。

【0005】

具体的には、以下に示す各状況に対して有効に機能できる技術が存在しない。

- (1) 「特定の物品」が「特定の位置」存在すること、又は「特定の個人」と「特定の物品」とを認証したい状況（特定の住所に対する配達の認証、物品受け渡しの認証など）
- (2) 「特定の位置」に「特定の人物」が存在することを認証したい状況（営業マンの巡回管理、オリエンテーリング状況管理など）
- (3) 個体（例えば、個人や物品等）の「特定の行動や移動」を認証したい状況（出張管理、産業廃棄物の廃棄管理、撮影データや録音データ等の著作証明など）
- (4) 一つ以上の「個体とその位置の認証」により、新たな2次的効果を得たい状況（特定の施設に対するリモート施錠管理など）

【0006】

なお、上記従来例1～従来例5においては、個人を特定し、その認証を行なうことは不可能である。また、従来例6や従来例7では、いわゆる「なりすまし」には対応できないため、提供される情報は、なりすました偽利用者に筒抜けとなる。例えば、上記のリモート施錠管理の場合であれば鍵が開いてしまう。

さらに、従来例8は、撮影者情報を添付することはできない。仮に、そのような装置を付け加えることによって画像データに撮像場所情報と撮影者情報を添付したとしても、容易に改変できるため、認証装置として機能し得ない。

そこで、本発明は、上記課題に鑑みてなされたものであり、特定の個人や特定の物品の存在の正当性について、確度の高い認証装置を提供することを目的とする。

【0007】

【課題を解決するための手段】

上記目的を達成するために、本発明に係る認証装置は、特定の個体を対象として、その正当性を認証する認証装置であって、前記個体から、当該個体を特徴づける第1対象情報を取得する対象情報取得手段と、前記取得された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、前記正当性が認証された個体が存在する位置を表わす位置情報を取得して前記対象情報に対応づける位置情報付加手段とを備える。

また、上記目的を達成するために、本発明に係る認証装置は、電波時計システムから前記個体が存在する時刻を表わす時間情報を取得して付加することを特徴とする。

【0008】

さらに、上記目的を達成するために、本発明に係る認証システムは、特定の個人及び当該個人が所持する特定の物品のうち、少なくとも一つの個体を対象として、当該個体の正当性と当該個体が実存することを認証するための認証サーバと、当該認証サーバにネットワークを介して接続されている認証用端末とからなる認証システムであって、前記認証用端末は、前記個体から、当該個体を特徴づける対象情報を取得する対象情報取得手段と、前記個体が存在する位置を表わす位置情報を取得する位置情報取得手段と、取得された前記対象情報及び前記位置情報を前記認証サーバに送信する送信手段とを備え、前記認証サーバは、前記認証用端末から対象情報及び位置情報とを受信する受信手段と、前記受信された対象情報に基づいて、前記個体の正当性を認証する対象情報認証手段と、前記受信された位置情報に基づいて、前記個体が存在する位置を認証する位置情報認証手段と、前記個体の正当性が認証され、前記位置情報が認証された場合に、前記個体が実存すると認証する実存認証手段とを備える。

【0009】

なお、上記目的を達成するために、本発明は、上記認証装置の特徴的な手段をステップとする認証方法として実現したり、それらのステップをパソコン等のコンピュータに実行させるプログラムとして実現することもできる。そして、そのようなプログラムをCD-ROM等の記録媒体やインターネット等の伝送媒体を介して流通させることもできる。

【0010】

【発明の実施の形態】

以下、本発明に係る実施の形態について、図面を参照しながら説明する。

(実施の形態1)

図1は、本実施の形態の一例であり、宅配会社の配達人が物品を配達する際に、本実施の形態における認証装置200を用いて種々の認証を行なう様子を示した図である。図1には、宅配会社100の配達人110が、配達先宅130において、受取人120に物品150を渡す様子が示されている。この際、配達人110は、認証装置200を用いて、配達人、物品、配達先及び配達時刻等の認証を行なう。

ここで、「認証」とは、行為や文書等が正当な行為者や正当な手続き等によって行なわれたことを証明することをいい、例えば、特定の個人であること、実在すること、正当な授受が行なわれたこと、内容の改竄がないことなどを証明する場合が該当する。

【0011】

具体的には、配達人110が物品150を受取人120に渡す際に、認証装置200を用いて配達人110の指紋を採取し、この指紋が認証装置200に予め登録されている配達人110の指紋と一致した場合に「配達人が認証された」ととする。さらに、物品150のバーコード151を読み取り、予めこのバーコードに対応付けられている住所152と、この場所でGPS衛星140を介して取得した位置情報とが一致した場合に「物品及び配達先が認証された」ととする。さらにまた、予め上記バーコードに対応付けられて登録されている配達時間帯の中に、配達時に取得（例えば、内蔵されている時計や電波時計等から取得）した時刻が入っている場合に「配達時刻が認証された」ととする。

【0012】

図2は、上記図1における認証装置200の外観図である。認証装置200は、物品150の配達時に配達人110の操作により、「配達人」、「物品」、「配達先」及び「配達時刻」について認証を行なうスタンドアロン型の端末であり、表示パネル220、赤外線ポート230、指紋読取センサ240、キーボード

250、メモリスロット260、バーコードリーダ270及びアンテナ280等が筐体210に格納されている。

表示パネル220は、例えば、液晶パネルであり、キーボード250を介してオペレータから受け付けた操作入力の内容や上記の認証結果の表示等を行なう。図2には、種々の認証結果や手続きの状況等の表示例が示されている(221～224)。

【0013】

赤外線ポート230は、IrDAの規格等に基づいて、赤外線を用いることによりPC(Personal Computer)など、他の情報端末とのデータ通信を可能とするための入出力ポートである。

指紋読取センサ240は、指紋を読み取るための静電容量方式又は光学式等のセンサであり、この上に置かれた指の指紋を取り込む。

【0014】

メモリスロット260は、例えば、SDメモリカード等の小型記憶媒体に対する読み出し／書き込みを行なうためのインターフェース装置である。例えば、この小型記憶媒体には、予め配達前に宅配会社500において、配達すべき物品のIDコード毎に、受取人の氏名及びその住所152、配達予定の配達人のIDコード及び配達予定時間帯等が予め記憶されている。なお、配達人のIDコードとその配達人の指紋データは、別途内蔵するメモリ(図示せず)に格納され、宅配会社100の管理者等によって登録／更新等が行なわれ、安全が確保されているものとする。

【0015】

バーコードリーダ270は、上記の配達される物品150に添付されているバーコード151を読み取るための(例えば、OCR型又はCCD型等の)装置である。

アンテナ280は、例えば、PHSや携帯電話の基地局(図示せず)又はGPS衛星140等から送信される位置情報や時間情報等を受信するためのアンテナである。

【0016】

図3は、上記図2の認証装置200の機能構成を示すブロック図である。図3に示されるように、認証装置200は、入力部10、表示部20、演算制御部30、対象情報処理部40、送受信制御部50、時間情報認証部60、位置情報処理部70、映像生成部80及び記憶部90等を備えている。

入力部10は、本装置200に必要なデータの取得及びオペレータからの操作入力を受け付ける部分であり、対象情報取得部11及びユーザ入力部12から構成されている。

対象情報取得部11は、上記図2における指紋読取センサ240やバーコードリーダ270を含み、認証の対象とする物（例えば、個人や物品など）から、それらを個別に識別することが可能な情報（以下、「対象情報」という。）を取得し、演算制御部30に送信する。

【0017】

ここで、個人を認証する場合の対象情報としては、オペレータから入力されたIDコードやパスワード、指紋読取センサ240等から入力される指紋データ、声紋データ、顔の特徴を表わした画像データ、虹彩データ、DNAデータなどがある。なお、これらの対象情報のうち、1つの対象情報によって認証を行なうこととしてもよいし、2以上の対象情報を組み合わせて、より高精度で認証を行なうこととしてもよい。一方、物品を認証する場合の対象情報としては、物品のIDコード（バーコードを含む。）や物品の特徴を表わした画像データなどがある。

【0018】

ユーザ入力部12は、上記図2におけるキーボード250に対応する部分であり、必要に応じてオペレータからIDコードやパスワード等のキーボード入力を受け付ける。

表示部20は、上記図2における表示パネル220を含み、ユーザ入力部12を介して入力された内容や認証結果の表示等を行なう。

【0019】

演算制御部30は、例えば、ROMやRAM等を備えるマイクロコンピュータなどであり、認証装置200全体の制御を行なう。さらに、演算制御部30は、

対象情報取得部11から対象情報を受信して対象情報処理部40に送信する。この場合、演算制御部30は、必要に応じて受信した対象情報をデータベースとして記憶部90に記憶する。さらにまた、演算制御部30は、内部に計時が可能なクロックを備えており、時間情報取得部61から要求があった場合は、その時刻を表わす時間情報を返す。なお、演算制御部30は、いわゆる電波時計を内蔵し、これに基づいて時間情報を送信することとしてもよい。

対象情報処理部40は、演算制御部30を介して受信した対象情報について、認証処理を行なったり、対象情報DB42に記憶されている対象情報の更新を行なう機能を有しており、対象情報認証部41、対象情報DB42及び対象情報更新部43から構成される。

【0020】

対象情報認証部41は、演算制御部30から受信した対象情報と対象情報DB42に予め記憶されている情報を照合し、一致／不一致等の判定を行ない、その結果を演算制御部30に通知する。例えば、対象情報取得部11において入力された配達人の指紋データと予め対象情報DB42に記憶されている指紋データとを照合し、一致するものがある場合は、その指紋データに対応する「配達人ID」を演算制御部30に通知し、一致しない場合は「該当者なし」を通知する。対象情報取得部11から、配達人の指紋データの以外のデータ、例えば、IDコードやパスワード、声紋データ、顔の特徴に関するデータ、虹彩データ及びDNAデータ等を入力し、これに基づいて予め登録されているデータとの照合を行ない、その結果を演算制御部30に通知することとしてもよい。

【0021】

対象情報DB42は、例えば、RAMやハードディスク等であり、個人や物品を識別するためのIDコードやパスワード、指紋データ、声紋データ、顔の特徴に関するデータ、虹彩データ及びDNAデータ等を記憶する。上記データの登録／更新等は、特定の者のみが実施することとし、安全が確保されているものとする。

対象情報DB更新部43は、演算制御部30の指示により、対象情報DB42に記憶されている対象情報の登録／更新等を行なう。

【0022】

送受信制御部50は、現在位置や現在時刻の特定に必要な位置情報や時間情報を取得するために、GPS衛星、PHS、携帯電話等との通信を行なう機能を有しており、GPSデータ受信部51、位置情報受信部52及びデータ送信部53を備える。

GPSデータ受信部51は、GPS衛星550から位置情報や時間情報を受信する。位置情報受信部52は、PHSや携帯電話の基地局からの位置情報や、パソコンからの位置情報などを受信する。データ送信部53は、上記図2における赤外線ポート230、及びPHSや携帯電話における送信制御回路等に対応する部分であり、演算制御部30から受信した認証結果等のデータをPCや他の携帯情報端末等に送信する。

【0023】

時間情報認証部60は、演算制御部30から受信した時間情報と記憶部90に予め記憶されている情報（例えば、上記の配達時間帯）とを照合し、その結果を演算制御部30に通知する。例えば、GPSデータ受信部51を介して取得された時間情報と予め記憶部90に記憶されている配達時間帯とを照合し、この配達時間帯に時間情報が示す時刻が含まれている場合は、「時間内配達」を演算制御部30に通知し、上記時刻が含まれていない場合は「時間外配達」を通知する。

【0024】

位置情報処理部70は、送受信制御部50及び演算制御部30を介して受信した位置情報と予め位置情報DB72に記憶されているデータを照合することにより位置の認証を行なう機能を有しており、位置情報生成認証部71、位置情報DB72及び位置情報DB更新部73から構成されている。

位置情報生成認証部71は、演算制御部30を介して受信した位置情報を、予め位置情報DB72に記憶されている位置情報に合わせて変換（例えば、経度／緯度を実際の住所に変換）し、変換後の位置情報と予め位置情報DBに記憶されている位置情報と照合し、一致／不一致を判定する。判定結果は、演算制御部30に通知する。

【0025】

位置情報DB72は、例えば、ハードディスクやRAM等であり、上記位置情報の変換を行なうためのデータが記憶されている。例えば、緯度／経度で表現されている位置情報を住所（〇〇県△△市・・等）に変換する（又はその逆の変換を行なう）ためのデータベースである。

位置情報DB更新部73は、演算制御部30の指示に従って、位置情報DB72の内容の更新等を行なう。

映像生成部80は、オペレータによって取得された映像（例えば、配達対象の物品の外観やIDコードなど）の映像データや、バーコードの読み取り結果等を記憶する。

【0026】

記憶部90は、上記図2におけるメモリスロット260や小型記憶媒体、RAM等であり、演算制御部30の指示により、上記のように、配達前に登録される配達すべき物品のIDコード毎の受取人の氏名及びその住所、予定配達人のIDコード及び配達予定時間帯や、認証結果として登録される物品IDコード毎の配達人ID、配達位置、配達日時などが記憶される。なお、上記小型記憶媒体は、SDカードやマルチメディアカードなどに代表される任意のメモリカードの他、フレキシブルディスク等であってもよい。

【0027】

図4～図6は、上記図3における対象情報DB42又は記憶部90に格納されるデータの構成例である。

図4は、対象情報DB42に格納される配達人指紋データ等の構成例である。図4に示されるように、配達人指紋データ403は、配達人ID401及び配達人氏名402に対応付けられて、予め（配達開始前に）対象情報DB42に格納される。なお、この指紋データの登録／更新等については、一部の担当者のみが行ない、配達人は、登録／変更等を行なうことができないこととする。

【0028】

図5は、記憶部90に格納される配達用データテーブルの構成例である。ここで、「配達用データテーブル」とは、未配達の物品に関する情報をまとめたテーブルであり、当日、配達が開始される前に登録される。図5に示されるように、

配達用データテーブル500には、物品ID501毎に、受取人氏名502、受取人住所503及び配達予定時間帯504が、予め（配達開始前に）記憶部90に格納される。なお、上記配達予定時間帯505の欄には、年月日を合わせて登録することとしてもよい。また、この配達用データの登録／更新等については、担当者が登録／変更等を行なうこととする。

【0029】

図6は、記憶部90に登録される配達完了時における認証結果データテーブルの構成例である。ここで、「認証結果データテーブル」とは、物品の配達に際して、種々の認証に必要な情報や認証結果をまとめたテーブルであり、配達完了時に格納される。図6に示されるように、認証結果データテーブル600としては、物品ID601毎に、配達人ID602、配達位置603、配達日時504及び受取人指紋データ605が、配達完了時に記憶部90に格納される。ここで、配達人ID602は、配達時に配達人の指紋データと予め登録されている指紋データとが一致した場合に、対応する配達人IDが記載される。また、経度と緯度で示される配達位置603及び配達日時604は、バーコードリーダ270によって物品IDが読み込まれた場合に、自動的にGPS衛星等から取得して格納される。受取人指紋データ605は、物品の配達を完了した確認として、受取人から取得する。

【0030】

次に、上記の宅配会社100の配達人110が、物品150を配達する場合において、認証装置200を用いて種々の認証を行なう場合の認証装置200の処理の流れについて説明する。

【0031】

図7は、本認証装置200の処理の様子を示したフローチャートである。

最初に、演算制御部30は、表示部20に、「配達人の指紋を入力して下さい。」等の表示を行ない（S701）、配達人からの指紋の入力を待つ（S702）。

指紋が入力されると、演算制御部30は、対象情報DB42を参照し、当該配達人が正当な配達人であるか否かを判別するように、対象情報認証部41に指示す

る。この場合、正当な配達人であると判別されると、当該配達人は「認証された」こととなる（S703）。

【0032】

次に、演算制御部30は、表示部20に、「物品のバーコードを入力して下さい。」等の表示を行ない（S704）、物品に添付されているバーコードの入力を待つ（S705）。バーコードが入力されると、演算制御部30は、対象情報DB42を参照し、当該物品が配達予定の物品であるか否かを判別するよう、対象情報認証部41に指示する。配達予定の物品であると判別されると、当該物品は「認証された」こととなる（S706）。

【0033】

さらに、演算制御部30は、表示部20に、「受取人の指紋を入力して下さい。」等の表示を行ない（S707）、受取人からの指紋の入力を待つ（S708）。指紋が入力されると、演算制御部30は、送受信制御部50に、位置情報及び時間情報を取得するように指示する（S709）。位置情報及び時間情報が取得されると、演算制御部30は、配達位置、配達時刻が正当か否かを判別するよう、位置情報処理部70及び時間情報認証部62に指示する（S710）。

さらに、演算制御部30は、上記の認証結果を表示部20に送信する（S711）。

【0034】

以上のように、本実施の形態の認証装置200によれば、予め登録され、その安全性が確保されているデータと動的に取得したデータとを照合してその正当性を判別するので、「特定の位置」に「特定の個体（人や物）」が「存在すること」や「正当な授受が行なわれたこと」等を認証することが可能となる。

なお、上記実施の形態では、「配達人の指紋」、「物品ID」、「受取人の指紋」の順で認証を行なったが、認証順序は任意である。また、個人を認証するための対象情報として指紋データを用いる例を示したが、指紋データに限るものではなく、上記のように、声紋データ、顔の特徴を示す画像データ、虹彩データ等を用いることとしてもよい。

【0035】

また、上記実施の形態の対象情報認証部41及び位置情報生成認証部71における認証方法は、一般的の認証手法を用いることができる。例えば、所定の認証機関が作成した認証実行コードを用いることもできる。また、後に述べるサーバから各端末（この場合は各認証装置）の認証用コードを所定の条件に沿って動的に制御し、認証精度を保つ（なりすましなどを防ぐ）ことも可能である。

【0036】

さらに、上記実施の形態において、物品150の認証に用いる対象情報は、バーコード151に限定するものではなく、物品を認証する任意の情報（外観の映像データ等）であってもよい。このとき、タグが物品Sに添付されていることを映像生成部80で画像として確認することもできる。これによって物品Sからタグが外れていないことなどを確認することが可能となる。

なお、物品Sの画像から直接、物品Sを認証することもできる。物品SがB氏のもとに届けられた際に、認証装置1によって、その場所と物品Sを認証することで確かにその場所に物品Sが届けられたことが証明される。

【0037】

例えば、前述のA氏がB氏への重要な物品Sの配達を配達会社D社に依頼した場合を考えると、B氏の認証と物品Sの認証を行なうことで、D社はA氏に対して「B氏に物品Sが渡ったこと」を証明することができる。D社の虚偽申告（実際には物品Sを渡していないにもかかわらず「渡した」と申告すること）や、なりすまし（B氏以外の人物がB氏に代わって物品Sを受け取ること）を防ぐことができ、D社としても、確実に荷物の配達を終えたことを証明できる。これは、配達証明郵便や、その他任意の「特定の人物」と「特定の物品」の認証によって意味をなす事象に応用できる。

【0038】

（実施の形態2）

上記の実施の形態1においては、スタンドアロンで使用する認証装置200について説明したが、本実施の形態では、ネットワークを介して構成される認証システム300について説明する。この認証システム300は、認証装置201から指紋データや位置情報等の認証に必要なデータを受信した認証サーバ310が

、これらのデータに基づいて種々の認証（例えば、出張として訪問した「訪問者」とその「訪問先」、「訪問時刻」等の認証等）を行なうシステムである。

なお、以下においては、上記実施の形態1と異なる構成について重点的に説明し、共通する構成については同一の符号を付して、その説明は省略することとする。

【0039】

図8は、本実施の形態における認証システム300のシステム構成図である。図8に示されるように、本システム300は、インターネット等のネットワーク320を介して認証装置201から認証サーバ310に対象情報を送信し、認証サーバ310が、受信した対象情報に基づいて認証を行なうものである。

認証装置201は、認証サーバ310に対象情報を送信するための端末であり、上記実施の形態1の認証装置200と同じ機能を有しているが、認証装置200における対象情報処理部40、時間情報認証部60及び位置情報処理部70を有していないてもよい。

【0040】

一方、認証サーバ310は、認証装置201から対象情報を受信し、この情報に基づいて、種々の認証を行なうサーバ（例えば、通信機能及びサーバ機能を有するパーソナルコンピュータ等）であり、上記認証装置200における演算制御部30、対象情報処理部40、時間情報認証部60及び位置情報処理部70を有する（図示せず）。

【0041】

図9は、認証システム300による管理対象の一例である出張の様子を示した図であり、出張における予定ルートと訪問予定時刻（図9では（）内に示されている。）とを表わした図である。図9に示されるように、社員901は、10時に会社910を訪問し、その後、13時に会社920、15時に会社930、16時に会社940を順次訪問することとする。その際、社員901は、それぞれの訪問先に到着時に、指紋データ、位置情報等を認証サーバ310に送信する。これにより、営業所900における管理者902は、「訪問者」、「訪問先」及び「訪問時刻」を認証する。

【0042】

図10は、上記認証サーバ310に格納される、社員901の出張予定を表わすデータを格納したテーブル（以下、「出張予定テーブル」という。）の構成例である。図10に示されるように、この出張予定テーブル1000は、訪問先会社名1001毎に、その会社の所在地1002、訪問予定者ID1003及び訪問予定日時1004を表わすデータが格納される。この出張予定テーブルは、社員901の出張前に、認証サーバ310の記憶部90に格納される。

【0043】

図11は、上記認証サーバ310に格納される、社員901の出張結果を表わすデータを格納するテーブル（以下、「出張結果テーブル」という。）の構成例である。図11に示されるように、この出張結果テーブル1100は、訪問先会社名1101毎に、訪問位置1102、訪問者ID1103、訪問日時1104を表わすデータ及び訪問者の指紋データ1105が登録される。この出張結果テーブルの各データは、社員901（又は認証用端末201のオペレータ）が出張先の会社に到着後（認証装置201から対象情報を受信し、その認証後）に、認証サーバ310の記憶部90に格納される。なお、図11において“-”は、その会社には未到着のため、未設定のデータであることを表わしている。

【0044】

図12は、社員901の出張時の認証サーバ310と認証装置201間における通信シーケンス図である。

まず、社員901の出張前に、出張予定テーブル1000に、必要なデータが登録される（S1201）。次に、社員901は、出張先の会社に到着すると到着処理として、自分の「指紋データ」、取得した「位置情報」及び「時刻情報」を認証サーバ310に送信する（S1202、S1203）。これにより、認証サーバ310は、受信した上記の情報に基づいて、認証処理として「訪問者」、「訪問先」及び「訪問時刻」の認証を行ない、出張結果テーブル1100に所定のデータを登録する（S1204）。

以下、予定に従って順次会社に到着する度に、上記の処理が繰り返される（S1205）。

【0045】

図13は、上記図12の認証用端末201における到着処理の様子を示すフローチャートである。

最初に、認証用端末201の演算制御部30は、表示部20に、「出張者の指紋を入力して下さい。」等の表示を行ない(S1301)、オペレータからの指紋の入力を待つ(S1302)。指紋が入力されると、演算制御部30は、指紋データを生成する(S1303)。

次に、演算制御部30は、送受信制御部50に、位置情報及び時間情報を取得するように指示する(S1304)。位置情報及び時間情報が取得されると、演算制御部30は、上記の指紋データ、位置情報及び時間情報を認証サーバ310に送信する(S1305)。

【0046】

図14は、上記図12における認証処理1204の様子を示すフローチャートである。

最初に、認証サーバ310の演算制御部30は、認証用端末201から出張人の指紋データ、位置情報及び時間情報を受信すると(S1401)、予め対象情報DB42に記憶されている訪問者の指紋データ、記憶部90に記憶されている所在地1002及び訪問予定日時1004に基づいて、それぞれ訪問者、訪問先及び訪問時刻を認証する(S1402～S1404)。なお、上記S1402～S1404の各処理の認証順序は図14の限りではなく任意である。

また、本認証システム300は、上記の出張管理に限らず、著作物における著作者等の認証や、施錠管理における担当者等を認証する場合に応用可能である。

【0047】

図15は、本認証システム300を用いて、写真の著作物における著作者と撮影場所等を認証する場合の認証サーバ310と認証用端末201間における通信シーケンス図である。

最初に、認証用端末201は、撮影者の操作によって写真のデータを取り込むと(S1501)、図13と同様の手順で取得された(“訪問者”を“撮影者”にして適用。)、写真データ、指紋データ、撮影した場所の位置情報及び撮影した

時刻の時間情報を認証サーバ310に送信する(S1502、S1503)。

【0048】

次に、認証サーバ310の演算制御部30は、認証用端末201から写真データ、指紋データ、位置情報等を受信すると、予め登録しておいた撮影者の指紋データに基づいて撮影者を認証する(S1504)。さらに、認証サーバ310の演算制御部30は、予め登録しておいた撮影予定場所を表わす情報に基づいて、撮影場所(撮影者の現在位置)を認証する(S1505)。

なお、上記の撮影対象から上記バーコードのように対象物を識別し得る情報を取得することができる場合は、併せてこの情報を認証サーバ310に送信して、より高い精度で認証を行なうこととしてもよい。

【0049】

図16は、本認証システム300を用いて、「ある施設の施錠管理者が、その施設内に作業者がいない場合に施錠を行なう場合」の、作業者とその場所等を認証する場合の認証サーバ310と認証用端末201間における通信シーケンス図である。この場合、作業者は、認証用端末201を所持しており、認証サーバ310は、管理センター(図示せず)内に設置されているものとする。さらに、施錠管理者自身が管理センター内にいる場合にのみ、その施設に対して施錠することが可能であるとする。

最初に、作業員が施設から退場すると、認証用端末201は、作業員から指紋の入力を受け付け(S1601)、位置情報及び時間情報を取得する(S1602)。さらに、認証用端末201は、取得した指紋データ及び位置情報等を認証サーバ310に送信する(S1603)。

【0050】

次に、管理センター内の認証サーバ310は、受信した作業員の指紋データ及び位置情報等に基づいて、作業員が施設内に居ないことを認証し(S1604、S1605)する。さらに、認証サーバ310は、管理者からの指紋データと位置情報及び時間情報を取得し、管理者が管理センター内に居ることを認証する(S1606、S1607)。以上の認証により、施設内に作業員が居ないことを確認すると(S1608)、認証サーバ310は、施設の施錠を行なうことが可

能となる(S 1 6 0 9)。

なお、上記のシステムは、作業員が複数の場合であっても、同様の認証を各作業員について繰り返すことによって、同様の施錠管理が可能である。

【0051】

以上のように、本実施の形態に係る認証システムを用いることにより、ネットワークを介して認証用端末から認証サーバに対象物とその位置情報等を送信し、認証サーバで認証を行なうので、遠隔地において、より確度の高いセキュリティシステムを構築することが可能となる。

なお、認証装置の内部に認証処理を高速化するために、上記の対象情報D Bや位置情報D B以外に、L U T : Logical Unit Table) を用いることとしてもよい。これを用いることにより、認証に必要なデータの入力を削減させることができるとなる。

【0052】

なお、複数の認証を重畠して行なうことにより、認証精度を高めることもできる。例えば、認証装置の誤認証率が、それぞれ1 0 0 0 分の1であった場合、2台の認証装置を用いて認証することにより、1 0 0 万分の1に誤認証率を下げることができる。

なお、上記の複数台の認証装置と同様に、一つの認証対象物、人に対して、複数の認証用データを用いることで認証精度を向上することもできる。

【0053】

さらには、2つの認証がともに承認された場合に限り、認証を有効にすることにより、物品受け渡しなどの際に勘合符がわりとして使用する（物品の受け渡しを行なう）こともできる。複数の認証用データを用いることによる機能は上記に限定されず、任意の機能実現に複数の認証用データを用いることができる。

なお、特定の認証装置の認証機能そのものを他の認証装置が認証することやサーバが認証することもできる。

【0054】

なお、認証装置は認証手段として秘密鍵や公開鍵、一方向性関数の逆演算の困難性に基づく暗号などの暗号技術や汎等によるD N A認証を用いてよい。

なお、認証方法が複数ある場合は、通信環境や装置の性能等などに応じて認証サーバが動的に選択し、その認証方法を認証用端末に通知することとしてもよい。

さらに、オペレータのパスワード等が第三者等に漏れてしまった場合に、例えば「パスワードが漏れている可能性があります。」など、オペレータに警告を提示するように構成してもよい。また、当該装置の使用を停止するように制御してもよい。

【0055】

【発明の効果】

以上のように、本発明に係る認証装置により、

(1) 「特定の物品」が「特定の位置」存在すること、又は「特定の個人」と「特定の物品」とを認証したい状況（特定の住所に対する配達の認証、物品受け渡しの認証など）

(2) 「特定の位置」に「特定の人物」が存在することを認証したい状況（営業マンの巡回管理、オリエンテーリング状況管理など）

(3) 個体（例えば、個人や物品等）の「特定の行動や移動」を認証したい状況（出張管理、産業廃棄物の廃棄管理、撮影データや録音データ等の著作証明など）

(4) 一つ以上の「個体とその位置の認証」により、新たな2次的効果を得たい状況（特定の施設に対するリモート施錠管理など）

といった各状況に対して、有効に機能する認証装置を提供することが可能となる。

【図面の簡単な説明】

【図1】

実施の形態1に係る、宅配会社の配達人が物品を配達する際における認証装置を用いて種々の認証を行なう様子を示した図である。

【図2】

図1における認証装置の外観図である。

【図3】

認証装置の機能構成を示すブロック図である。

【図4】

対象情報DBに格納される配達人指紋データ等の構成例である。

【図5】

記憶部に格納される配達用データテーブルの構成例である。

【図6】

記憶部に登録される配達完了時における認証結果データテーブルの構成例である。

【図7】

認証装置の処理の様子を示したフローチャートである。

【図8】

実施の形態2における認証システムのシステム構成図である。

【図9】

認証システムによる管理対象の一例である出張の様子を示した図である。

【図10】

認証サーバに格納される、社員の出帳予定を表わす出張予定テーブルの構成例である。

【図11】

認証サーバに格納される、社員の出張結果を表わすデータを格納する出張結果テーブルの構成例である。

【図12】

社員の出張時の認証サーバと認証装置間における通信シーケンス図である。

【図13】

図12の認証用端末における到着処理の様子を示すフローチャートである。

【図14】

図12における認証処理の様子を示すフローチャートである。

【図15】

認証システムを用いて、写真の著作物における著作者と撮影場所等を認証する場合の認証サーバと認証用端末間における通信シーケンス図である。

【図16】

認証システムを用いて、「ある施設の施錠管理者が、その施設内に作業者がいない場合に施錠を行なう場合」の、作業者とその場所等を認証する場合の認証サーバと認証用端末間における通信シーケンス図である。

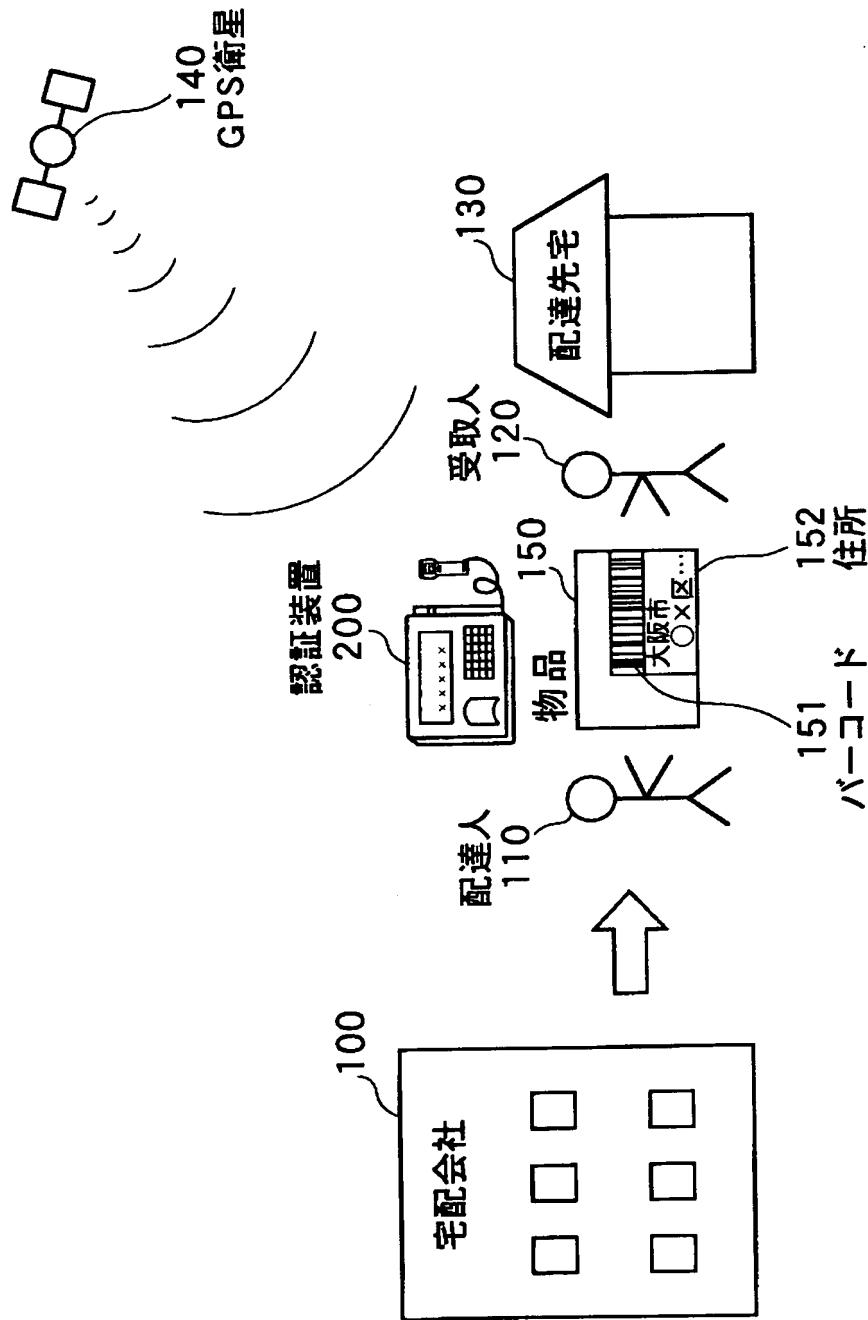
【符号の説明】

1 0	入力部
1 1	対象情報取得部
1 2	ユーザ入力部
2 0	表示部
3 0	演算制御部
4 0	対象情報処理部
4 1	対象情報認証部
4 2	対象情報DB
4 3	対象情報DB更新部
5 0	送受信制御部
5 1	GPSデータ受信部
5 2	位置情報受信部
5 3	データ送信部
6 0	時間情報認証部
7 0	位置情報処理部
7 1	位置情報生成認証部
7 2	位置情報DB
7 3	位置情報DB更新部
8 0	映像生成部
9 0	記憶部
2 0 0	認証装置
2 0 1	認証用端末
2 1 0	筐体
2 2 0	表示パネル

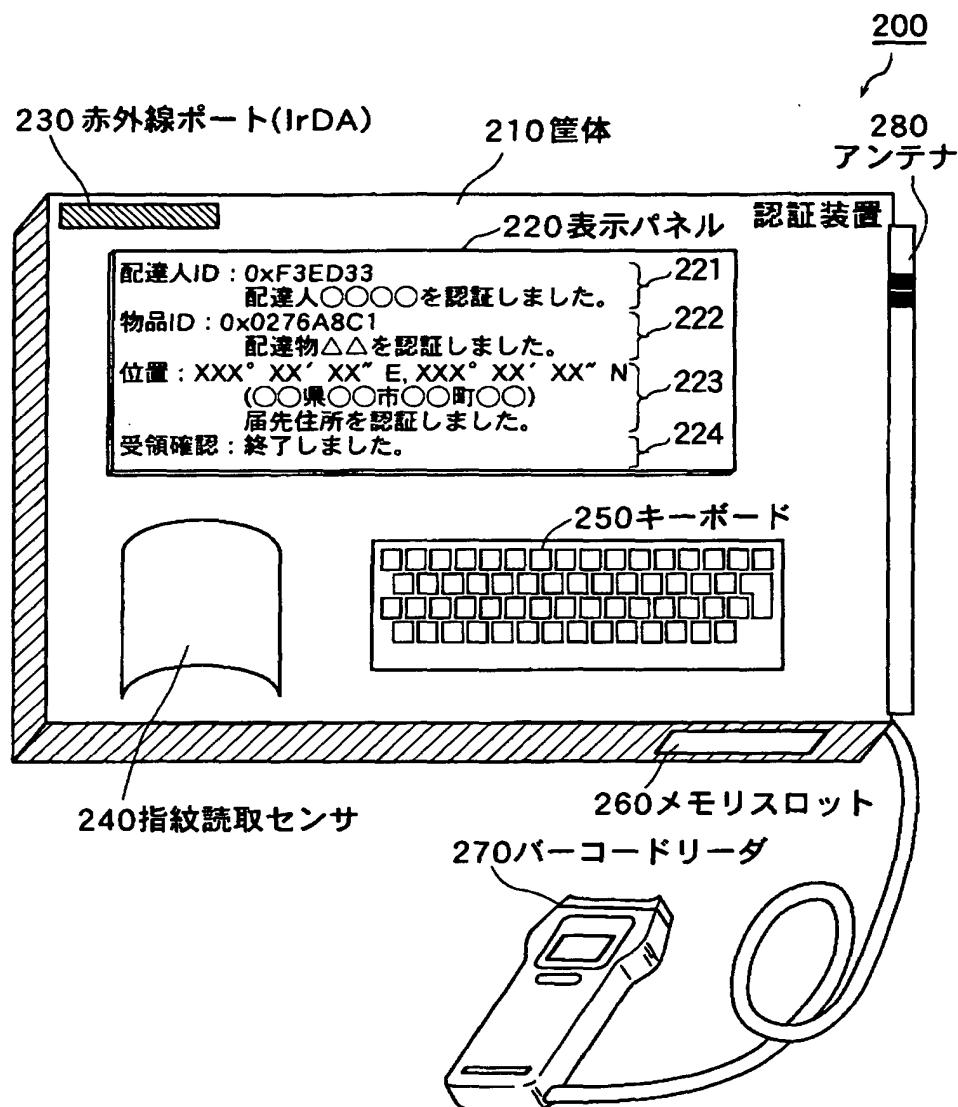
230 赤外線ポート
240 指紋読取センサ
250 キーボード
260 メモリスロット
270 バーコードリーダ
280 アンテナ
300 認証システム
310 認証サーバ
320 ネットワーク

【書類名】図面

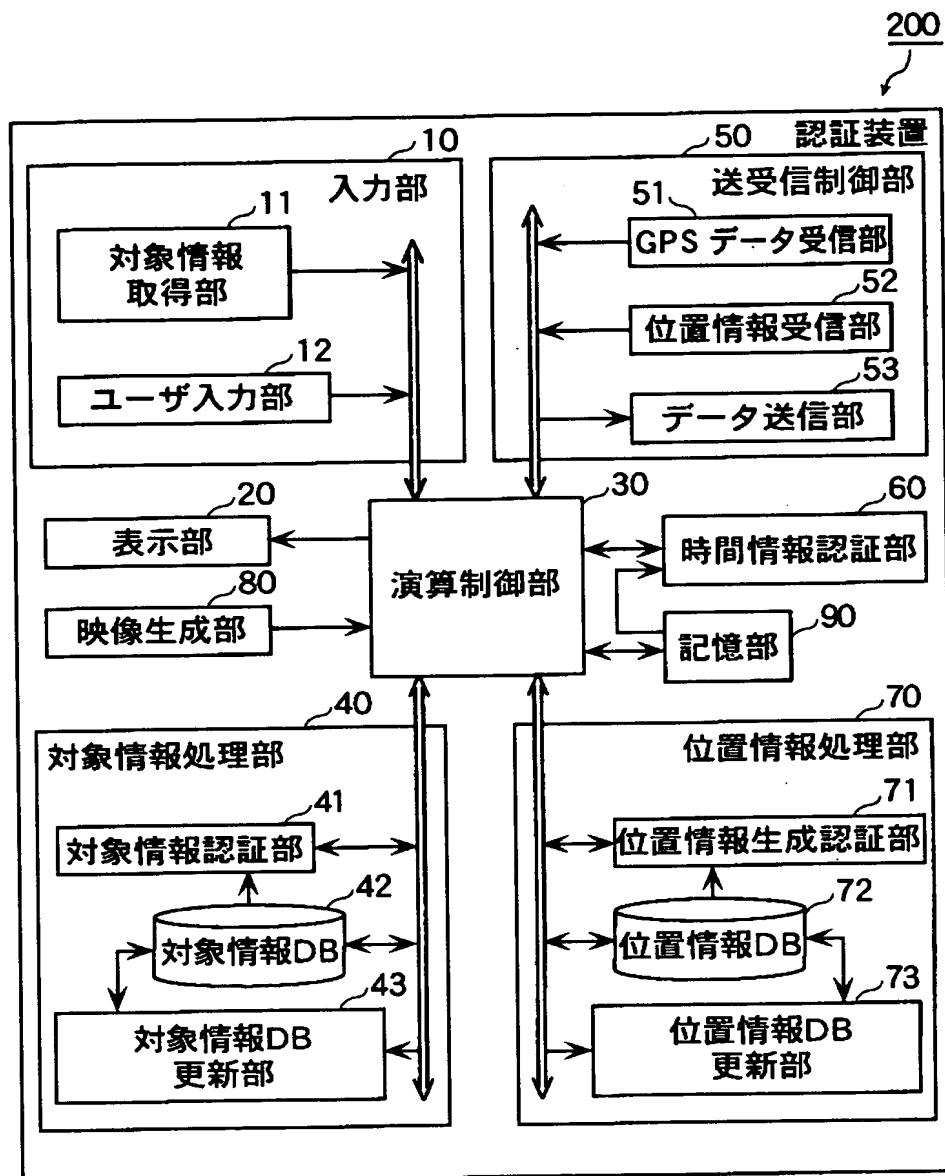
【図1】



【図2】



【図3】



【図4】

配達人ID 401	配達人氏名 402	配達人指紋データ 403
0xF3ED33	佐藤 一子	* * *
0xM4AH75	鈴木 次郎	* * *
0xM8CB18	高橋 三郎	* * *
⋮	⋮	⋮
⋮	⋮	⋮

【図5】

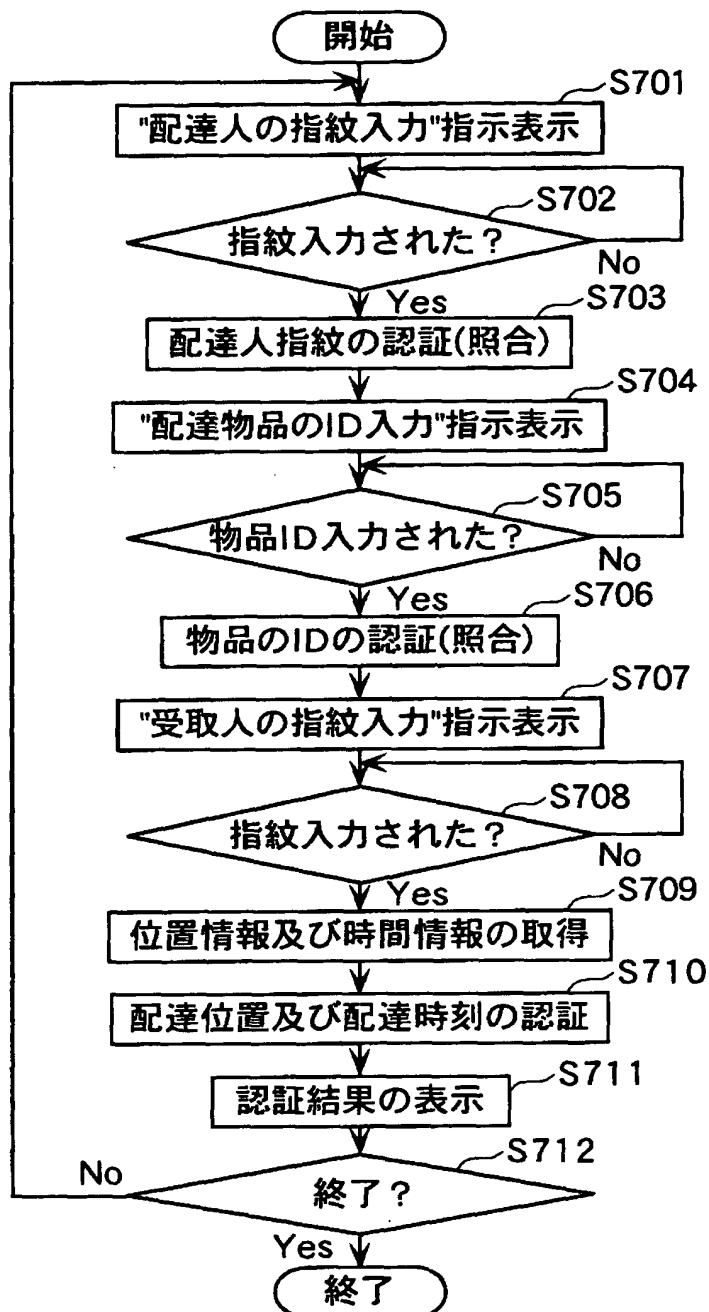
500

501 物品ID	502 受取人氏名	503 受取人住所	504 予定配達人ID	505 配達予定時間帯
0xE276A8C1	山田 史郎	兵庫県神戸市	0xF3ED33	9時～12時
0xA103B379	青藤 吾郎	大阪府大阪市	0xF3ED33	15時～18時
0xD625F418	伊藤 重郎	京都府京都市	0xF3ED33	12時～15時
⋮	⋮	⋮	⋮	⋮
⋮	⋮	⋮	⋮	⋮

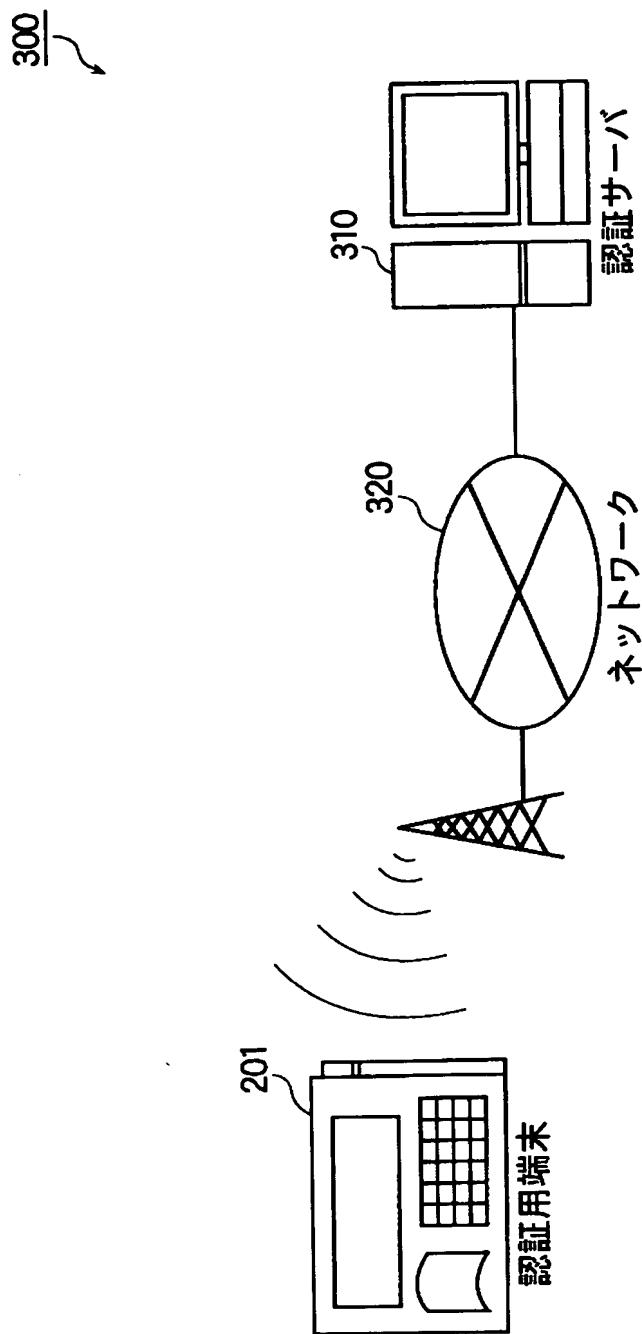
【図6】

物品ID	配達人ID	配達位置	配達日時	受取人指紋データ
0xE276A8C1	0xF3ED33	XXX° XX' XX'' E, XXX° XX' XX'' N	2002.07.07/10:01	* * *
0xA103B379	-	-	-	-
0xD625F418	-	-	-	-
...

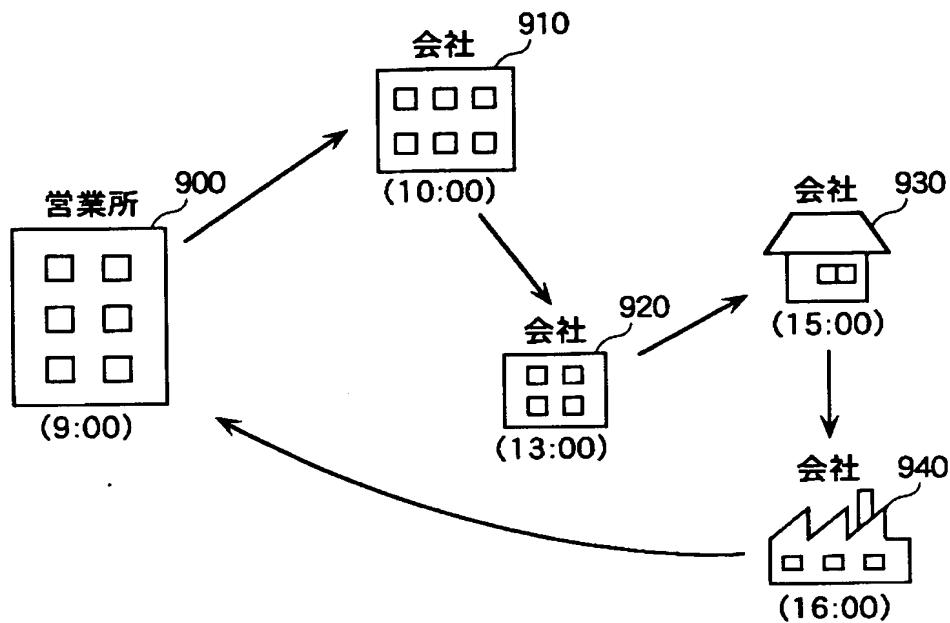
【図7】



【図8】



【図9】



【図10】

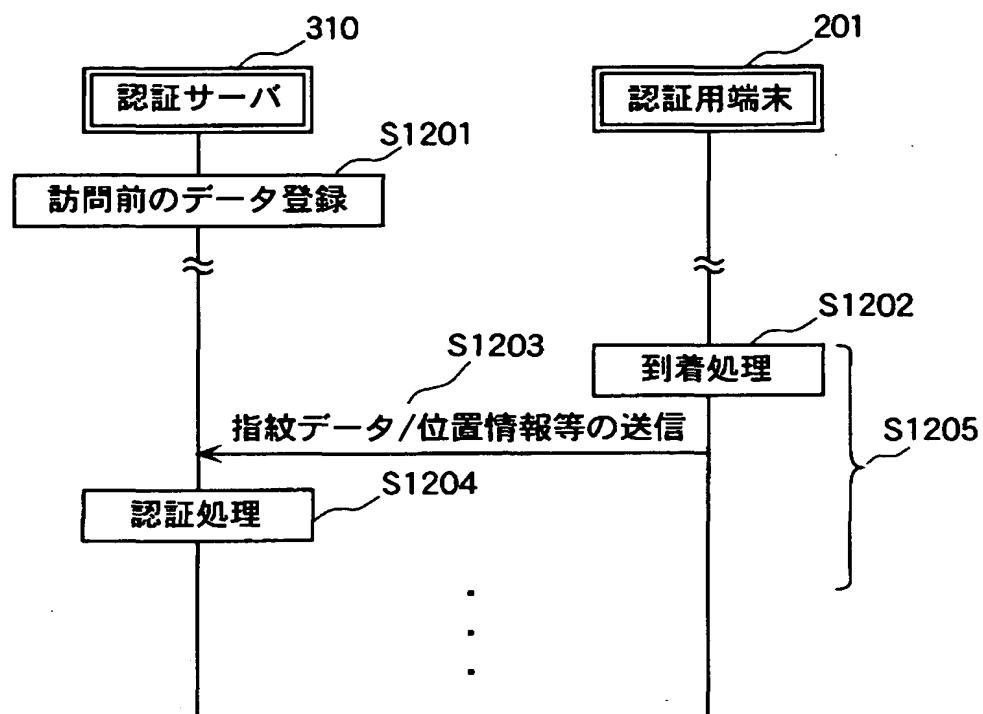
訪問先会社名	所在地	訪問予定者ID	訪問予定日時
A会社	滋賀県大津市	0xF3ED33	2002 09 09/10 00
B会社	京都府京都市	0xF3ED33	2002 09 09/13 00
C会社	大阪府大阪市	0xF3ED33	2002 09 09/15 00
D会社	大阪府大阪市	0xF3ED33	2002 09 09/16 00

【図11】

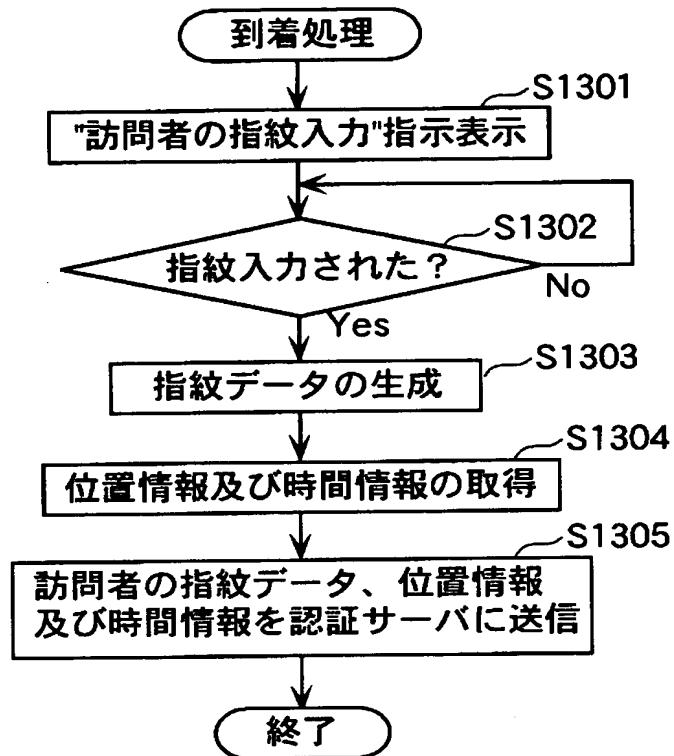
1100

訪問先会社名	訪問位置	訪問者ID	訪問日時	訪問者の指紋データ
A会社	XXX° XX' XX" E, YY° YY' YY" E,	0xF3ED33	2002 09 09/09:55	***
B会社	—	0xF3ED33	2002 09 09/12:58	***
C会社	—	—	—	—
D会社	—	—	—	—

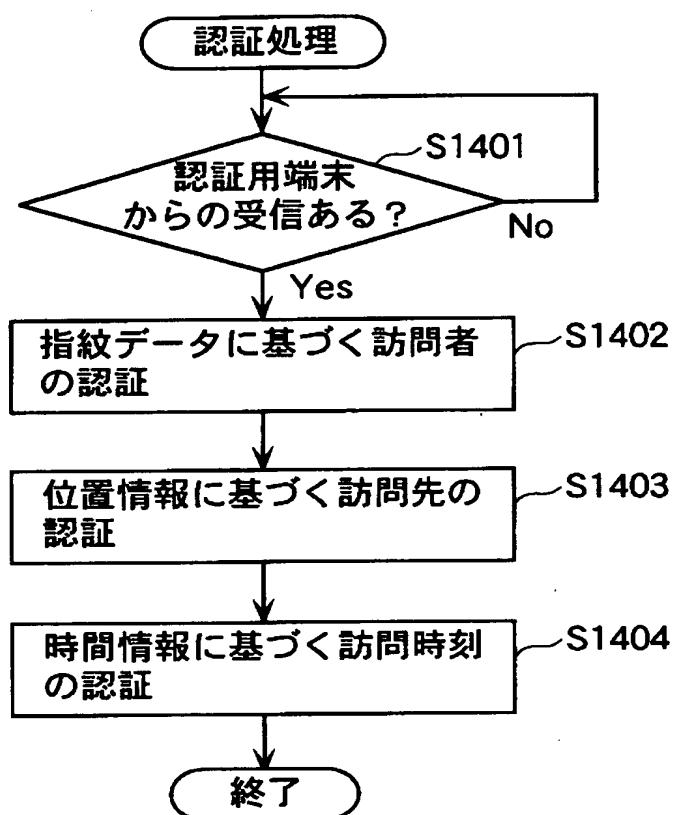
【図12】



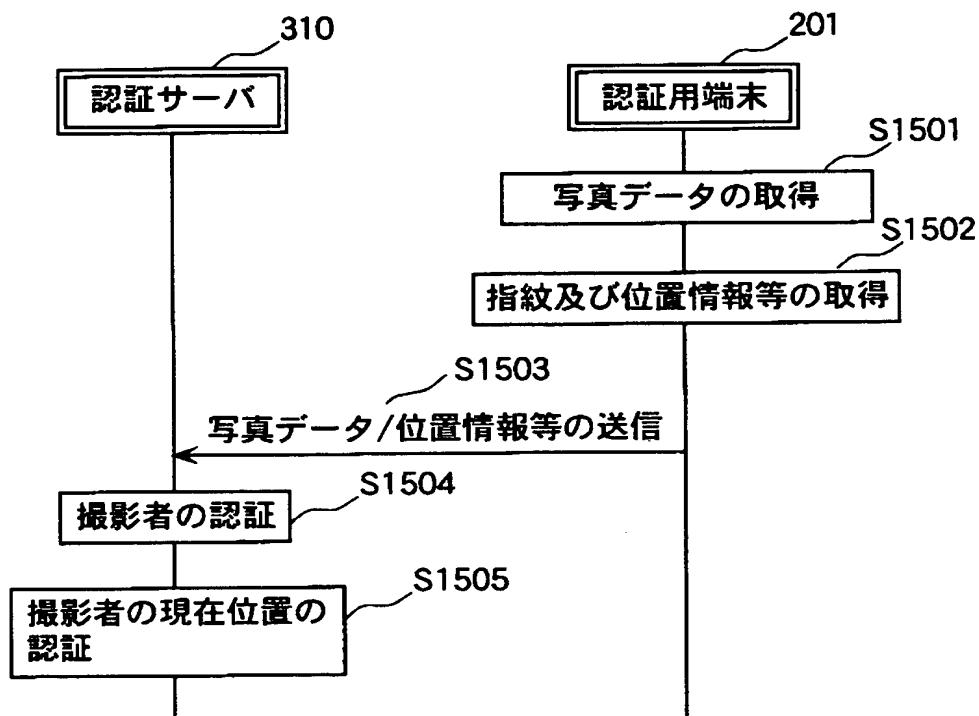
【図13】



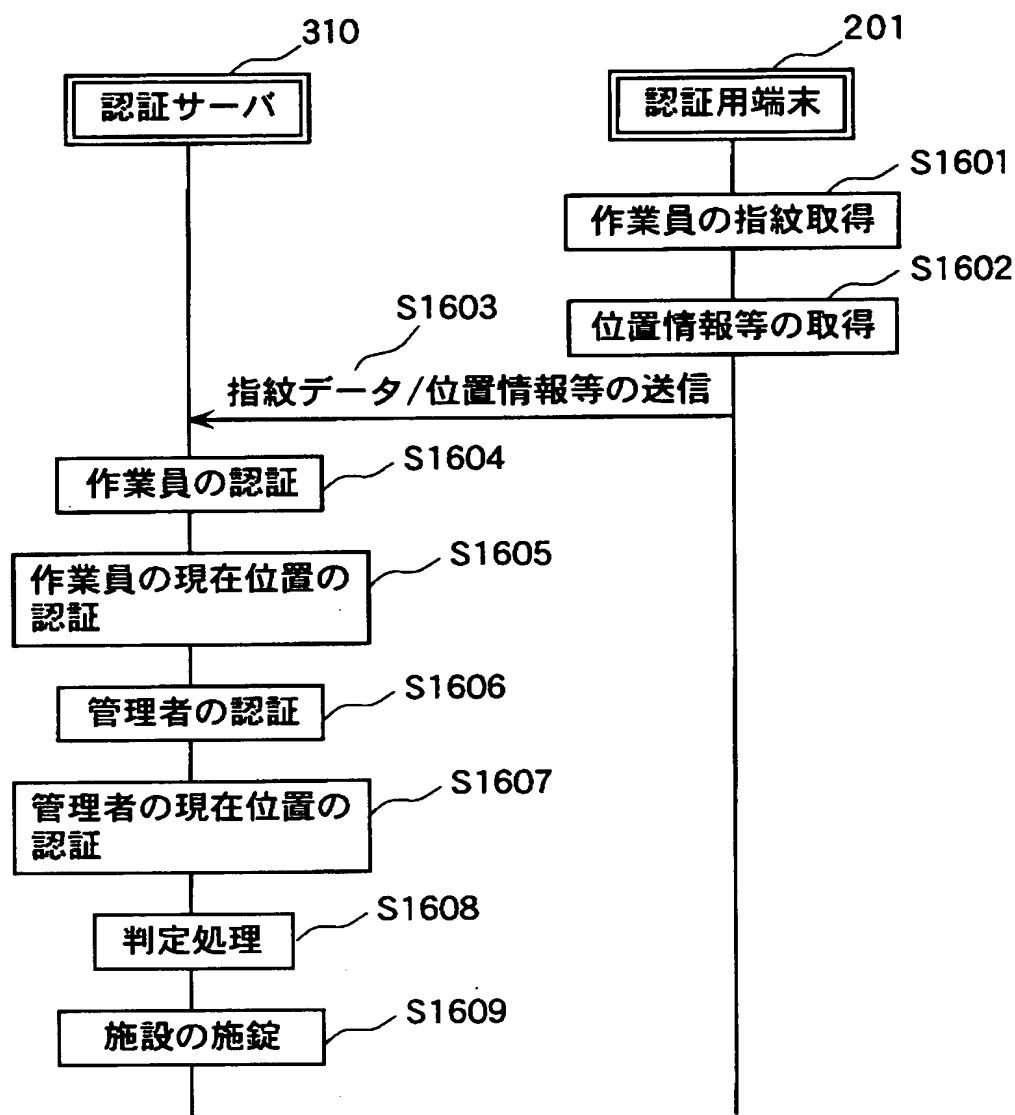
【図14】



【図15】



【図16】



【書類名】 要約書

【要約】

【課題】 「特定の位置」に「特定の個人（又は物品）」が存在することを認証し得る認証装置を提供する。

【解決手段】 対象情報取得部11やユーザ入力部12により、対象物の認証に必要な情報（対象情報）を取得する。取得された対象情報は、演算制御部30を介して認証対象情報処理部40に入力され、対象情報認証部41によって個人、物品等が認証される。この認証の際、対象情報DB42を利用する。また、GPSデータ受信部51や位置情報受信部52により、現在位置の特定に必要な位置情報を取得する。この位置情報は、GPS衛星、携帯電話やPHSの基地局等から取得する。位置情報認証部71は、取得された位置情報と予め記憶部90に記憶されている情報に基づいて、位置の認証を行なう。この認証の際、位置情報DB72を利用する。

【選択図】 図3

認定・付加情報

特許出願の番号	特願2002-226532
受付番号	50201151529
書類名	特許願
担当官	小野寺 光子 1721
作成日	平成14年 8月 5日

＜認定情報・付加情報＞

【提出日】 平成14年 8月 2日

次頁無

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社